In the Specification:

Please substitute the following paragraphs for the corresponding paragraphs beginning at the indicated location in the specification as originally filed.

Page 5, line 16+:

However, while this system facilitates administrator operations and removal of obsolete or duplicated access authorizations, neither it nor other known systems significantly reduce the overall complexity of administration of access authorizations as secure web systems become large in terms of number of resources, number of users or both. Further, the number of resources to which access authorizations pertain may be greatly increased by division of such resources in order to provide different levels of security for different portions thereof. Additionally, there has been much recent development in the technology of database architecture and management techniques as well as a trend toward archival documentation of database content; both tending to increase the number of substitutions of databases and correspondingly increased numbers of access authorization changes on large systems.

a1

Page 7, line 18+:

In order to accomplish the above and other objects of the invention, the method and system of the invention provide profiles, one or more of which can be associated with each user to specify one or more resources to which access may be granted to a user to whom that profile is assigned. Lists of users, profiles and resources are maintained in an access control program executable on a network server, and may be freely created and edited under supervision of a system administrator and the profiles provide an

a2

association between the users and resources that the users are authorized to access and the mode of that ~~assess~~ access. Thus changes in accessible resources may be automatically propagated through the access authorization information and associated with users while accommodating unique user authorizations. Further, access authorizations are automatically carried out upon completion of any editing of the lists of access authorization information. Users are authenticated at the server level and authorized requests of authenticated users are directed to the target resource.

a2

Page 13, line 26+:

Referring again to Figure 1A, it should be appreciated that the architecture of the system 10 in accordance with the invention is divided into three levels. At the level indicated by reference numeral 12, users are assigned one or more security profile(s), indicated by pointers/arrows to the level indicated by reference numeral 14. It is through the profile(s) that a user gains entry into one or more databases (or assets), resources or directories 193, 194, 195, 199, 220 at the level indicated by reference numeral 16 to which the secure web server allows access. An exemplary user table including corresponding profiles and other information by which the user is authenticated is illustrated in Figure 13.

a3

Page 28, line 32+:

The password, if required at this point, is checked, and if valid, the user is allowed access to the data base (or asset), as shown at 124. If either userID and/or password is not valid, then the user is informed of the fact, and, returned to START (125), data base selection (1) , userID entry (7), or Exit. The choice between these alternatives is not important

a4

a4

to the practice of the invention in accordance with its basic principles but generally would be chosen as an incident of the security level to be provided and different options could be provided in accordance with the protection to be accorded to particular assets.